Twisted Edwards curve and its group of points over finite field F_p

U. V. Skruncovich
NTUU, Kiev, Ukraine
julian.skrunkovich@gmail.com

R. V. Skuratovskii
NPU, Kiev, Ukraine
ruslan@imath.kiev.ua

We consider the conditions of supersingularity of Edwards curve [1–3]. A normalization of this curve was constructed by us in projective form. We denote twisted Edwards curve having coefficients a and d as $E_{a,d}$. It was found the mistake in conditions of supersingularity for this curve in theorem 3 of article [4]. More particularly if $p \equiv -3(\bmod 8)$ there is no degenerated twisted pair of curves as it states in [4]. Also if condition $p \equiv \pm 7(\bmod 8)$ holds then the orders of correspondent curves are such $N_{E_2} = N_{E_{2^{-1}}} = p-3$ that are not equal $p+1$ as it states in [4]. For instance if $p = 31$ then $N_{E_2} = N_{E_{2^{-1}}} = 28 = 8 \cdot 3 + 7 - 3$.

The main result of this paper is the theorem.

Theorem 1. *If $p \equiv 3 \pmod 4$ and p is prime, then numbers of points on $x^2 + y^2 = 1 + 2x^2y^2$ and on $x^2 + y^2 = 1 + 2^{-1}x^2y^2$ over F_p are equal $N_{E_{1,2}} = N_{E_{1,2^{-1}}} = p+1$ when $p \equiv 3(\bmod 8)$ and $N_{E_2} = N_{E_{2^{-1}}} = p-3$ when $p \equiv 7(\bmod 8)$.*

There are two fundamental points [6] $((0, \pm 1), (\pm\sqrt{a}, 0))$ on $E_{a,d}$. The interesting relations between points of $E_{a,d}$ were found.

Theorem 2. *For every no fundamental point (x, y) of $E_{a,d}$ holds the condition $\left(\frac{1-\ ax^2}{p}\right)\left(\frac{1-y^2}{p}\right) = \left(\frac{a-d}{p}\right)$.*

If a is a quadratic residue over F_p then it exists the isomorphism between Edwards curve $E_{1,d}$ and twisted Edwards curve $E_{a,d}$, which is given by the mapping $X \mapsto \sqrt{a}x, Y \mapsto y$. This fact and the theorem 1 lead us to a condition of supersingularity of $E_{a,d}$.

Remark. *Point of order 8 exists on $E_{a,d}$ if and only if point of order 4 exists on $E_{a,d}$ and following conditions holds $(\frac{\frac{1}{d}(1\pm\sqrt{1-\frac{d}{a}})}{p}) = 1$, $(\frac{\frac{a}{d}(1\pm\sqrt{1-\frac{d}{a}})}{p}) = 1$, $(\frac{a}{p}) = 1$, $(\frac{1-\frac{d}{a}}{p}) = 1$.*

References

[1] E. K. Alekseev, I. V. Oshkin, V. O. Popov, S. V. Smishliev, About perspectives of using twisted Edwsrds curves in Gost R 34.10-2012 *Proceedings of the XVI conference "RusCrypto 2014"*.

[2] Daniel J. Bernstein, Peter Birkner, Marc Joye, Tanja Lange, Christiane Peters, Twisted Edwards Curves. *IST Programme under Contract IST-2002-507932 ECRYPT, and in part by the National Science Foundation under grant ITR-0716498* (2008) 1–17.

[3] Hisil Huseyin, Koon-Ho Wong Kenneth, Carter Gary, *Twisted Edwards Curves Revisited. ASIACRYPT* LNCS 5350 (2008) 326–343.

[4] A. V. Bessalov, O. V. Tsygankova, Correlation of big order points sets of the Edwards curves over prime field. *Information protection* **17(1)** (2015) 73–79.

[5] Lidl Nideraiter, Introduction to Finite Fields and their Applications. By Rudolf Lidl. By Harald Niederreiter. *Encyclopedia of Mathematics and its Applications* **20** Cambridge University Press (1996) 755.

[6] W. Fulton, Algebraic curves. *An Introduction to Algebraic Geometry* **3** (2008) 121.